

MINIMUM DISTANCE FOR TORIC COMPLETE INTERSECTION CODES

IVAN SOPROUNOV

ABSTRACT. In this paper we give lower bounds for the minimum distance of evaluation codes constructed from complete intersections in toric varieties. This generalizes the results of Gold–Little–Schenck and Ballico–Fontanari who considered evaluation codes on complete intersections in the projective space.

1. INTRODUCTION

This work is inspired by the results of Gold, Little and Schenck [10] and Ballico and Fontanari [2] on evaluation codes on complete intersections in the projective space. Examples of evaluation codes include Reed–Muller codes on points in affine and projective spaces and Goppa codes on points in algebraic curves. Here is a general definition. Let X be an algebraic variety over a finite field \mathbb{F}_q and let $S = \{p_1, \dots, p_N\}$ be a finite set of \mathbb{F}_q -rational points of X . Furthermore, let \mathcal{L} be a finite dimensional space of regular functions over \mathbb{F}_q defined on an open subset of X containing S . This defines an *evaluation map*

$$\text{ev}_S : \mathcal{L} \rightarrow (\mathbb{F}_q)^N, \quad f \mapsto (f(p_1), \dots, f(p_N)).$$

Its image is a linear code $\mathcal{C}_{S, \mathcal{L}}$ of block length N . In the situation when X is a projective toric variety, the set S is the algebraic torus $(\mathbb{F}_q^*)^n$, and \mathcal{L} is the space of linear sections of a Cartier divisor on X we obtain what is called a *toric code*. In this case \mathcal{L} is spanned by monomials whose exponents are lattice points in a convex lattice polytope. The minimum distance for toric codes was studied in [13, 21, 20, 22, 24, 25].

Duursma, Rentería, and Tapia-Recillas considered the situation when $X = \mathbb{P}^n$, the set S is an arbitrary zero-dimensional complete intersection in $\mathbb{P}^n(\mathbb{F}_q)$, and $\mathcal{L} = \mathcal{L}_a$ is the space of homogeneous polynomials of degree a . Their paper [6] is concerned with computing the dimension of the corresponding evaluation codes $\mathcal{C}_{S, \mathcal{L}_a}$. Later Gold, Little, and Schenck [10] found a very nice application of the Cayley–Bacharach theorem that gave a lower bound for the minimum distance of $\mathcal{C}_{S, \mathcal{L}_a}$, generalizing the 2-dimensional result of Hansen [11]. They showed that the minimum distance satisfies

$$d(\mathcal{C}_{S, \mathcal{L}_a}) \geq s - a + 2,$$

where $s = \sum_{i=1}^n d_i - (n+1)$ and d_1, \dots, d_n are the degrees of the polynomials defining S . Ballico and Fontanari [2] then gave a significantly better bound

$$d(\mathcal{C}_{S, \mathcal{L}_a}) \geq n(s - a) + 2,$$

which holds for complete intersections S satisfying a “generality” condition: no $n+1$ points of S lie on a hyperplane in \mathbb{P}^n .

Partially supported by NSA Young Investigator Grant H98230-10-1-0163.

In this paper we combine the two situations: X is a projective toric variety, S is a zero-dimensional complete intersection in X , and \mathcal{L} is a space of global sections of a Cartier divisor on X . The corresponding evaluation code we call a *toric code on complete intersection*. We give two lower bounds for the minimum distance of such codes: for sets S with and without a “generality” condition. Our bounds generalize the ones in [10] and [2]. Although we largely used methods from these papers, the difficulty is that no analog of the Cayley–Bacharach theorem for toric varieties is currently known. It turned out that the Toric Euler–Jacobi theorem (Theorem 2.4) on global residues (which can be thought of as a weak toric analog of the Cayley–Bacharach theorem, see Corollary 2.5) provides enough information for applications to evaluation codes.

In our exposition we decided to use not the language of toric geometry but rather the more explicit language of Laurent polynomial systems and Newton polytopes. The relationship between the two is discussed in Section 2.3. Section 2 gives the necessary preliminaries and states the Toric Euler–Jacobi theorem and its immediate applications. Section 3 contains the main results on the minimum distance of toric complete intersection codes: Theorem 3.2 does not use any additional assumptions, and Theorem 3.8 assumes a certain “generality” property of S . We give geometric conditions on the Newton polytopes of polynomials defining S (Theorem 3.9) which guarantee that this property holds when the coefficients of the polynomials are generic. The paper concludes with applications and concrete examples in Section 4 and remarks about further work.

I thank Ștefan Tohaneanu for several fruitful discussions about evaluation codes on complete intersections and Jan Tuitman for answering questions about Bernstein’s theorem in positive characteristic.

2. PRELIMINARIES

2.1. Evaluation Codes. In this section we will define evaluation codes we will be dealing with throughout the paper. First let us introduce some standard definitions and notation from the theory of Newton polytopes. Let \mathbb{K} be a field and $\overline{\mathbb{K}}$ be its algebraic closure. Consider a Laurent polynomial $f \in \mathbb{K}[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$. Its *Newton polytope* $P(f)$ is the convex hull of the exponent vectors of the monomials appearing in f . Thus we can write

$$f = \sum_{a \in P(f) \cap \mathbb{Z}^n} c_a t^a, \quad \text{where } t^a = t_1^{a_1} \cdots t_n^{a_n}, \quad c_a \in \mathbb{K}.$$

Given a face Q of $P(f)$ the *restriction* f^Q is the Laurent polynomial

$$f^Q = \sum_{a \in Q \cap \mathbb{Z}^n} c_a t^a.$$

Next we define evaluation codes slightly adapted to our situation (see [12, 19, 28] for a general definition). Choose a finite subset $S = \{p_1, \dots, p_N\}$ of $(\mathbb{K}^*)^n$ and a finite-dimensional subspace \mathcal{L} of $\mathbb{K}[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$. Define the *evaluation map*

$$\text{ev}_S : \mathcal{L} \rightarrow \mathbb{K}^N, \quad f \mapsto (f(p_1), \dots, f(p_N)).$$

The image of ev_S is a linear code, called the *evaluation code*, which we denote by $\mathcal{C}_{S, \mathcal{L}}$.

In the paper we will be dealing with evaluation codes $\mathcal{C}_{S, \mathcal{L}}$ where \mathcal{L} is a space of Laurent polynomials and S is the solution set of a Laurent polynomial system satisfying certain assumptions which we describe below.

Fix a collection of n -dimensional convex lattice polytopes P_1, \dots, P_n in \mathbb{R}^n and let $P = P_1 + \dots + P_n$ be their Minkowski sum. Consider n Laurent polynomials f_1, \dots, f_n over \mathbb{K} with Newton polytopes P_1, \dots, P_n such that the system $f_1 = \dots = f_n = 0$ satisfies the following.

Assumptions:

- (1) the system is *non-degenerate* with respect to P , i.e. for every proper face $Q \subset P$ the restricted system $f_1^{Q_1} = \dots = f_n^{Q_n} = 0$ has no solutions in $(\overline{\mathbb{K}}^*)^n$, where $Q = Q_1 + \dots + Q_n$, for unique faces $Q_i \subset P_i$;
- (2) the solution set $S \subset (\overline{\mathbb{K}}^*)^n$ of the system consists of \mathbb{K} -rational points;
- (3) at each $p \in S$ the collection (f_1, \dots, f_n) forms a system of local parameters, i.e. the 1-forms df_1, \dots, df_n are linearly independent at p .

Before describing the space \mathcal{L} we need to set some notation. For any set $A \subset \mathbb{R}^n$ we use $A_{\mathbb{Z}}$ to denote the set of lattice points in A , i.e. $A_{\mathbb{Z}} = A \cap \mathbb{Z}^n$. Also, we let P° denote the interior of the polytope $P = P_1 + \dots + P_n$. Now let A be any subset of P° . Define

$$\mathcal{L}(A) = \text{span}_{\mathbb{K}}\{t^a \mid a \in A_{\mathbb{Z}}\} \subset \mathbb{K}[t_1^{\pm 1}, \dots, t_n^{\pm 1}].$$

Definition 2.1. Let S be the solution set of a system $f_1 = \dots = f_n = 0$ with n -dimensional Newton polytopes P_1, \dots, P_n satisfying (1)–(3) above. Let set A lie in the interior P° of $P = P_1 + \dots + P_n$. The evaluation code $\mathcal{C}_{S, \mathcal{L}(A)}$ is called a *toric complete intersection code*. We will denote it the simply by \mathcal{C}_A . Furthermore, $d(\mathcal{C}_A)$ will denote the minimum distance (the minimum weight) of \mathcal{C}_A .

Remark 2.2. Although we are not assuming that A is a convex polytope (we are not even assuming that A is a convex set) all our results below depend on $A_{\mathbb{Z}}$ rather than A itself. In fact, the bounds we prove in Section 3 will not change if one replaces A with the convex hull of $A_{\mathbb{Z}}$.

2.2. The Toric Euler–Jacobi theorem. Here we discuss the toric analog of the Euler–Jacobi theorem (Theorem 2.4) and its consequences. This theorem was first discovered by Khovanskii (see [16]) over the field of complex numbers. In [17], Section 14 the first part of the theorem is proved over arbitrary algebraically closed field. In [14] the second part of the theorem is proved over fields of positive characteristic under the condition that the P_i have the same normal fan. The general case is currently unknown in positive characteristic and we hope to address it on a subsequent paper.

Definition 2.3. Let $f_1, \dots, f_n \in \mathbb{K}[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$ be Laurent polynomials. The Laurent polynomial

$$J_f^{\mathbb{T}} = \det \left(t_j \frac{\partial f_i}{\partial t_j} \right)$$

is called the *toric Jacobian* of f_1, \dots, f_n .

It is easy to see that the Newton polytope $P(J_f^{\mathbb{T}})$ of the toric Jacobian lies in $P = P_1 + \dots + P_n$, where $P_i = P(f_i)$. Also, assumption (3) in Section 2.1 implies $J_f^{\mathbb{T}}(p) \neq 0$ for every $p \in S$.

Theorem 2.4. [16] *Let S be the solution set of a system $f_1 = \dots = f_n = 0$ with n -dimensional Newton polytopes P_1, \dots, P_n satisfying (1)–(3) above. Let $P = P_1 + \dots + P_n$ be the Minkowski sum. Then*

- (1) for any $h \in \mathcal{L}(P^\circ)$ we have $\sum_{p \in S} h(p)/J_f^\mathbb{T}(p) = 0$;
- (2) for any function $\phi : S \rightarrow \mathbb{K}$ with $\sum_{p \in S} \phi(p) = 0$ there exists $h \in \mathcal{L}(P^\circ)$ such that $\phi(p) = h(p)/J_f^\mathbb{T}(p)$ for every $p \in S$.

Here are a few immediate corollaries from the theorem.

Corollary 2.5. *Any $h \in \mathcal{L}(P^\circ)$ which vanishes at $|S| - 1$ points of S must vanish at all points of S .*

Corollary 2.6. *If $|S| > 1$ then the minimum distance of \mathcal{C}_{P° is at least 2.*

Proof. Indeed, by part (2) of Theorem 2.4 there exist $h \in \mathcal{L}(P^\circ)$ that are not identically zero on S . Also they have at most $|S| - 2$ zeroes by Corollary 2.5. \square

The next theorem is also a consequence of Theorem 2.4 and can be thought of as a solution to the sparse polynomial interpolation problem.

Theorem 2.7. [23] *Let S be as in Theorem 2.4 and suppose $\text{char } \mathbb{K}$ does not divide the normalized mixed volume of the P_i . Then for any function $\phi : S \rightarrow \mathbb{K}$ there is a polynomial $g \in \mathcal{L}(P)$ such that $g(p) = \phi(p)$ for every $p \in S$. Moreover, g can be chosen to be of the form $g = h + cJ_f^\mathbb{T}$ for some $h \in \mathcal{L}(P^\circ)$ and a constant $c \in \mathbb{K}$.*

The following definition from classical algebraic geometry is directly related to polynomial interpolation.

Definition 2.8. We say that a finite set of points $T \subset (\mathbb{K}^*)^n$ imposes independent conditions on a space of Laurent polynomials \mathcal{L} if the evaluation map $\text{ev}_T : \mathcal{L} \rightarrow \mathbb{K}^{|T|}$ is surjective.

In the light of this definition Theorem 2.7 produces the following property of the solution set S .

Corollary 2.9. *Let S be as in Theorem 2.4. Then S imposes independent conditions on the space $\mathcal{L}(P)$.*

This can be slightly refined. According to the second statement of Theorem 2.7, the corollary still holds if we replace $\mathcal{L}(P)$ with $\mathcal{L}(\bar{P})$, where $\bar{P} = P^\circ \cup P(J_f^\mathbb{T})$.

The next result, known as Bernstein's theorem, provides the size of the solution set S for systems $f_1 = \dots = f_n = 0$ satisfying assumptions (1)–(3).

Theorem 2.10. [1] *Let S be the solution set of a system $f_1 = \dots = f_n = 0$ with Newton polytopes P_1, \dots, P_n satisfying assumptions (1)–(3). Then $|S|$ equals the normalized mixed volume $V(P_1, \dots, P_n)$ of the Newton polytopes.*

The original Bernstein's proof in [1] uses the homotopy continuation method and is valid over the field of complex numbers. Kushnirenko in [18] gave an algebraic proof which works over any algebraically closed field regardless of the characteristic. A similar argument also appears in [29], Section 6.

2.3. Relation to Toric varieties. Here we will show how our problem can be reformulated in the language of toric geometry. Let $X = X_\Sigma$ be a projective simplicial toric variety over \mathbb{K} of dimension n , defined by a complete rational simplicial fan $\Sigma \subset \mathbb{R}^n$. Each ray $\rho \in \Sigma(1)$ is generated by a primitive lattice vector $v_\rho \in \mathbb{Z}^n$ and corresponds to a torus-invariant prime divisor D_ρ on X . A *semi-ample* divisor D on X is a torus-invariant Cartier divisor

$D = \sum_{\rho \in \Sigma(1)} a_\rho D_\rho$ for which the corresponding line bundle $\mathcal{O}(D)$ is generated by global sections. This implies that the set

$$P_D = \{u \in \mathbb{R}^n \mid \langle u, v_\rho \rangle \geq -a_\rho, \rho \in \Sigma(1)\}$$

is a lattice polytope in \mathbb{R}^n (see [8], Section 3.4). Also the space of global \mathbb{K} -sections of $\mathcal{O}(D)$ is isomorphic to $\mathcal{L}(P_D)$ in our notation in Section 2.1.

Now fix n semi-ample divisors D_1, \dots, D_n on X and let $P_i = P_{D_i}$ be the corresponding lattice polytopes. For every $1 \leq i \leq n$ let f_i be a sections of the line bundle $\mathcal{O}(D_i)$. The assumptions (1)–(3) in Section 2.1 imply that f_1, \dots, f_n define a zero-dimensional complete intersection S in X , the intersection is transversal, lies in the dense orbit of X and consists of \mathbb{K} -rational points.

Now for any Laurent polynomial h consider the differential n -form

$$\omega_h = \frac{h}{f_1 \cdots f_n} \frac{dt_1}{t_1} \wedge \cdots \wedge \frac{dt_n}{t_n}.$$

It has poles on the zero set of the f_i , and at every $p \in S$ the local (Groethendieck) residue $\text{res}_p(\omega_h)$ is defined (see [9]). When the collection (f_1, \dots, f_n) forms a system of local parameters at p we have $\text{res}_p(\omega_h) = h(p)/J_f^{\mathbb{T}}(p)$. The sum of the local residues over $p \in S$ is the *global residue* $\text{Res}_f(h)$ of h with respect to $f = (f_1, \dots, f_n)$. In these terms the first statement of Theorem 2.4 says that the global residue of any $h \in \mathcal{L}(P^\circ)$ equals zero. The global residue is closely related to the toric residue defined by Cox in [5] and subsequently studied in [3, 4, 23]. The evaluation codes we consider here are essentially the same as the toric residue codes studied by Akhtar and Joshua in [14].

3. BOUNDS FOR THE MINIMUM DISTANCE

Recall that the evaluation code \mathcal{C}_A is constructed by choosing a subset A of P° . Note that lattice translations of A , i.e. translations by lattice vectors, result in equivalent codes, so the minimum distance $d(\mathcal{C}_A)$ is independent of such translations. Instead $d(\mathcal{C}_A)$ depends on “how big” A is with respect to P° .

In our first result (Theorem 3.2) we measure this by the number of “primitive” simplices Δ_i one can add to A and still stay in P° , after a possible lattice translation. We say that a simplex Δ is *primitive* if $\Delta = \text{conv.hull}\{0, v_1, \dots, v_n\}$, where $\{v_1, \dots, v_n\}$ is a basis for \mathbb{Z}^n .

The following simple lemma will be used throughout the paper.

Lemma 3.1. *Let B be a lattice set which generates \mathbb{Z}^n . Then any $m+1$ points in $(\mathbb{K}^*)^n$ impose independent conditions on the space $\mathcal{L}(mB)$.*

Proof. We may assume that B contains the origin. Let $\{v_1, \dots, v_n\} \subseteq B$ be a basis for \mathbb{Z}^n and let $s = t^M = (t^{v_1}, \dots, t^{v_n})$ be the corresponding automorphism of $(\mathbb{K}^*)^n$. Now let $T = \{p_0, \dots, p_m\}$ be any subset of $m+1$ points in $(\mathbb{K}^*)^n$. We need to construct a polynomial in $\mathcal{L}(mB)$ which vanishes at $T \setminus \{p_0\}$ and is not zero at p_0 . Let $T^M = \{p_0^M, \dots, p_m^M\}$ be the image of T under the automorphism, so T^M consists of $m+1$ distinct points. Now for every $1 \leq i \leq m$ choose a linear function $l_i(s)$ such that $l_i(p_i^M) = 0$ and $l_i(p_0^M) \neq 0$. Note that $l_i(t^M)$ lies in $\mathcal{L}(B)$. Then the polynomial $\prod_{i=1}^m l_i(t^M)$ lies in $\mathcal{L}(mB)$ and satisfies the required property. \square

Theorem 3.2. *Let S be the solution set of a system $f_1 = \dots = f_n = 0$ satisfying assumptions (1)–(3) above. Let A be any set such that $A + \Delta_1 + \dots + \Delta_l \subseteq P^\circ$ up to a lattice translation, where each Δ_i is a primitive simplex. Then $d(\mathcal{C}_A) \geq l + 2$.*

Proof. The proof is by induction on l . For $l = 0$ it is the statement of Corollary 2.6. For $l > 0$ take $h \in \mathcal{L}(A)$ which vanishes on a set $T \subset S$ of size $|S| - d(\mathcal{C}_A)$, but which is not identically zero on S . Since $A \subset P^\circ$ we have $d(\mathcal{C}_A) \geq 2$, by Corollary 2.6. Thus there exist distinct points $p, q \in S \setminus T$. By Lemma 3.1 with $m = 1$, one can choose $g \in \mathcal{L}(\Delta_l)$ such that $g(p) = 0$ and $g(q) \neq 0$. Then $hg \in \mathcal{L}(A + \Delta_l)$, vanishes on $T \cup \{p\}$, but is not identically zero on S . Therefore $d(\mathcal{C}_{A+\Delta_l}) < d(\mathcal{C}_A)$. On the other hand $A + \Delta_l$ satisfied the inductive hypothesis, so $d(\mathcal{C}_{A+\Delta_l}) \geq l + 1$ and the theorem follows. \square

Next theorem provides a certain reciprocity between two sets A, B whose sum lies in P° .

Theorem 3.3. *Let S be the solution set of a system $f_1 = \dots = f_n = 0$ satisfying assumptions (1)–(3) above. Let A and B be two subsets of \mathbb{R}^n such that $A + B \subseteq P^\circ$. If any $T \subseteq S$ of size m imposes independent conditions on the space $\mathcal{L}(B)$ then $d(\mathcal{C}_A) \geq m + 1$.*

Proof. We need to show that any $h \in \mathcal{L}(A)$, not identically zero on S , vanishes at no more than $|S| - m - 1$ points of S . Assume there exists $h \in \mathcal{L}(A)$ and a subset $Z \subset S$ of size $|S| - m$ such that h vanishes on Z , but $h(p) \neq 0$ for some $p \in S$. By our assumption $S \setminus Z$ imposes independent conditions on $\mathcal{L}(B)$, so there exists $g \in \mathcal{L}(B)$ such that g vanishes at every point of $S \setminus (Z \cup \{p\})$, but not at p . Now the polynomial hg belongs to $\mathcal{L}(A + B) \subseteq \mathcal{L}(P^\circ)$ and vanishes at every point of S but not at p , which contradicts Corollary 2.5. \square

Remark 3.4. Consider a special case: $X = \mathbb{P}^n$, f_1, \dots, f_n are homogeneous polynomials of degrees d_1, \dots, d_n ; and $\mathcal{L}(A)$ and $\mathcal{L}(B)$ are subspaces of homogeneous polynomials of degrees a and $s - a$, respectively, where $s = \sum_{i=1}^n d_i - (n + 1)$. In this case Theorem 3.3 follows from the Cayley–Bacharach theorem (see [7]) and serves as the main tool in the proofs of the results of [10] and [2]. We would like to point out that no toric analog of the Cayley–Bacharach theorem is currently known, however, the Toric Euler–Jacobi theorem is sufficient for our application to toric complete intersection codes.

In what follows we will consider solution sets $S \subset (\mathbb{K}^*)^n$ satisfying one additional assumption.

Assumption:

- (4) There exists an n -polytope Q such that any $|Q_{\mathbb{Z}}|$ points of S impose independent conditions on $\mathcal{L}(Q)$. In other words, for any subset $T \subset S$ of size $|Q_{\mathbb{Z}}|$ the evaluation map $\text{ev}_T : \mathcal{L}(Q) \rightarrow \mathbb{K}^{|Q_{\mathbb{Z}}|}$ is an isomorphism.

Example 3.5. Suppose $X = \mathbb{P}^n$ and $Q = \Delta$ is the standard n -simplex, i.e. the convex hull of the origin and the n standard basis vectors. Then (4) is equivalent to saying that no $n + 1$ points of S lie on a hyperplane. Complete intersections in \mathbb{P}^n with this “generality” assumption were considered in [2].

The assumption (4) allows us to obtain better bounds on the minimum distance of the codes \mathcal{C}_A , as was suggested by Ballico and Fontanari in [2] in the case of the projective space. In fact, their approach generalizes to arbitrary toric varieties. We will begin with a toric analog of the Horace Lemma.

Proposition 3.6. *Let $T \subset (\mathbb{K}^*)^n$ be a finite subset and A a bounded subset of \mathbb{R}^n . Consider a hypersurface H in $(\mathbb{K}^*)^n$ defined by $h \in \mathcal{L}(Q)$. If $T \cap H$ imposes independent conditions on $\mathcal{L}(A + Q)$ and $T \setminus (T \cap H)$ imposes independent conditions on $\mathcal{L}(A)$ then T imposes independent conditions on $\mathcal{L}(A + Q)$.*

Proof. Take any point $p \in T$. If $p \notin H$ then there exists $g \in \mathcal{L}(A)$ which does not vanish at p , but vanishes at all the other points of $T \setminus (T \cap H)$. Then the polynomial $f = gh \in \mathcal{L}(A + Q)$ vanishes at all points of $T \setminus \{p\}$. Also $f(p) = g(p)h(p) \neq 0$ since $p \notin H$.

Now if $p \in H$ then there exists $f_1 \in \mathcal{L}(A + Q)$ which does not vanish at p , but vanishes at all the other points of $T \cap H$. Consider the function $\phi : T \setminus (T \cap H) \rightarrow \mathbb{K}$ given by $q \mapsto f_1(q)/h(q)$. We know that there exists $g \in \mathcal{L}(A)$ such that $g(q) = \phi(q)$ for any $q \in T \setminus (T \cap H)$. Put $f = f_1 - gh$. Clearly $f \in \mathcal{L}(A + Q)$ and f vanishes at every point of T except at p . \square

Proposition 3.7. *Let S be the solution set of a system $f_1 = \dots = f_n = 0$ satisfying assumptions (1)–(4). Then, for any $k \geq 0$, any subset $T \subseteq S$ of size $|T| = (|Q_{\mathbb{Z}}| - 1)k + 1$ imposes independent conditions on $\mathcal{L}(kQ)$.*

Proof. The proof is by induction on k . For $k = 0$ we have $T = \{p\}$ which imposes independent conditions on the space $\mathcal{L}(kQ) \cong \mathbb{K}$.

For $k > 0$ choose $T' \subset T$ of size $m = |Q_{\mathbb{Z}}| - 1$. Since $m < |Q_{\mathbb{Z}}| = \dim \mathcal{L}(Q)$ there exists a non-zero polynomial $h \in \mathcal{L}(Q)$ which vanishes on T' . Moreover, $T' = S \cap H$, where H is the hypersurface defined by h . Indeed, if $S \cap H$ contains a point p not in T' then the evaluation map $\text{ev}_{T' \cup \{p\}} : \mathcal{L}(Q) \rightarrow \mathbb{K}^{m+1}$ is degenerate which contradicts the assumption (4). Clearly, since $T' \subset T \subset S$ we have $T' = S \cap H = T \cap H$.

Now $T \setminus T'$ has size $m(k - 1) + 1$ and by induction imposes independent conditions on $\mathcal{L}((k - 1)Q)$. Also by (4) the set T' imposes independent conditions on $\mathcal{L}(Q)$ and hence on $\mathcal{L}(kQ)$ as $Q \subset kQ$ up to a lattice translation. It remains to apply Proposition 3.6. \square

Theorem 3.8. *Let S be the solution set of a system $f_1 = \dots = f_n = 0$ satisfying assumptions (1)–(4). Let A be any set such that $A + kQ \subset P^\circ$ up to a lattice translation, for some $k \geq 0$. Then*

$$d(C_A) \geq (|Q_{\mathbb{Z}}| - 1)k + 2.$$

Proof. The theorem follows from Proposition 3.7 and Theorem 3.3 where we put $m = (|Q_{\mathbb{Z}}| - 1)k + 1$. \square

Our next goal is to give a geometric condition on the polytopes P_1, \dots, P_n and Q that produce systems satisfying assumption (4) if the coefficients are generic elements of $\overline{\mathbb{K}}$.

Theorem 3.9. *Let Q be a lattice n -polytope such that $Q_{\mathbb{Z}}$ generates \mathbb{Z}^n . Suppose $V(P_1, \dots, P_{n-1}, Q) \geq |Q_{\mathbb{Z}}|$ and $(|Q_{\mathbb{Z}}| - 1)Q \subset P_n$. Then the solution set of any system $f_1 = \dots = f_n = 0$ with Newton polytopes P_1, \dots, P_n and generic coefficients satisfies assumption (4).*

Proof. Let $m = |Q_{\mathbb{Z}}| - 1$. Let Γ_i be the hypersurface in $(\overline{\mathbb{K}}^*)^n$ defined by f_i . Consider the curve $C = \Gamma_1 \cap \dots \cap \Gamma_{n-1}$ in $(\overline{\mathbb{K}}^*)^n$. Let V consist of all ordered collection (p_0, \dots, p_m) of regular points in C such that $\{p_0, \dots, p_m\}$ do not impose independent conditions on $\mathcal{L}(Q)$. In other words,

$$V = \{T = (p_0, \dots, p_m) \in C_{\text{reg}}^{m+1} \mid \text{ev}_T : \mathcal{L}(Q) \rightarrow (\overline{\mathbb{K}}^*)^{m+1} \text{ is degenerate}\},$$

where by abuse of notation we denote by T both the ordered collection (p_0, \dots, p_m) and the set $\{p_0, \dots, p_m\}$. The set V is algebraic with a dense open subset $V_0 \subset V$ consisting of points of V for which the map ev_T has one-dimensional kernel.

First we will show that $\dim V = m$. Indeed, every $T \in V_0$ defines a unique hypersurface H , defined by a polynomial in $\mathcal{L}(Q)$, such that the corresponding set T lies in $C \cap H$. We obtain a map $\pi : V_0 \rightarrow \mathbb{P}\mathcal{L}(Q)$. On the other hand, by Bernstein's theorem (see Theorem 2.10) any generic hypersurface H with Newton polytope Q satisfies $|C \cap H| = V(P_1, \dots, P_{n-1}, Q) \geq m + 1$, so the image of π is dense in $\mathbb{P}\mathcal{L}(Q)$. Clearly, the fibers $\pi^{-1}(H)$ are finite, so we get $\dim(V) = \dim(V_0) = \dim(\pi(V_0)) = \dim(\mathbb{P}\mathcal{L}(Q)) = m$.

Now we will show that choosing a generic f_n with Newton polytope P_n produces $S = C \cap \Gamma_n$ which satisfies assumption (4). For this consider the set

$$W = \bigcup_{T \in V} W_T, \quad \text{where } W_T = \{f \in \mathcal{L}(P_n) \mid f \text{ vanishes on } T\}.$$

Clearly, every f_n in the complement of W produces such S (we also must avoid those f_n which have zero coefficients corresponding to the vertices of P_n), so we need to show W has positive codimension in $\mathcal{L}(P_n)$. Indeed, according to our assumption $mQ \subset P_n$, so every set of $m + 1$ points in S imposes independent conditions on $\mathcal{L}(mQ)$ (by Lemma 3.1) and hence on $\mathcal{L}(P_n)$. Therefore the codimension of every subspace W_T equals $m + 1$. Thus W is a vector bundle with m -dimensional base and codimension $m + 1$ fibre, so W has codimension one. \square

Remark 3.10. Note that the condition $(|Q_{\mathbb{Z}}| - 1)Q \subset P_n$ in Theorem 3.9 can be replaced with $P_1 + \dots + P_{n-1} + Q \subset P_n$ (or with its refinement as in the remark after Corollary 2.9). Indeed, consider $T \in V$. By definition there exists a hypersurface H defined by a polynomial in $\mathcal{L}(Q)$ such that $T \subseteq C \cap H$. By Corollary 2.9, $C \cap H$ imposes independent conditions on the space $\mathcal{L}(P_1 + \dots + P_{n-1} + Q)$. Therefore T imposes independent conditions on $\mathcal{L}(P_n)$. The rest is as in the above proof.

4. EXAMPLES

In this section we put several applications of the results of the previous section as well as provide specific examples of toric complete intersection codes over finite fields.

We start by showing how Theorem 3.2 and Theorem 3.8 recover the results of Gold-Little-Schenck and Ballico-Fontanari [10, 2].

Example 4.1. Let S be a zero-dimensional smooth complete intersection in \mathbb{P}^n given by n homogeneous polynomials F_1, \dots, F_n over \mathbb{K} . Suppose S lies in $\mathbb{P}^n(\mathbb{K})$. Up to a projective change of coordinates we may assume that S lies in the algebraic torus $(\mathbb{K}^*)^n$. Rewriting F_i in the affine coordinates for $(\mathbb{K}^*)^n$ we obtain a polynomial f_i with Newton polytope $P_i = d_i \Delta$ where Δ is the standard n -simplex and $d_i = \deg(F_i)$. It is easy to see that S satisfies the assumptions (1)–(3) in Section 2.1.

Now let $s = \sum_{i=1}^n d_i - (n + 1)$ and let $A = a\Delta$ for some $1 \leq a \leq s$. Notice that $\mathcal{L}(A)$ is the space of polynomials of total degree at most a . We are going to apply Theorem 3.2 with $l = s - a$ and all the Δ_i being simply Δ . Clearly, $A + \Delta_1 + \dots + \Delta_n$, which equals $s\Delta$, lies in the interior of $P = (\sum_{i=1}^n d_i)\Delta$. Therefore, by Theorem 3.2, $d(\mathcal{C}_A) \geq s - a + 2$. This is the result of [10].

Next suppose S satisfies assumption (4) with $Q = \Delta$. As pointed out before this means that no $n+1$ points of S line in a hyperplane in \mathbb{P}^n . Applying Theorem 3.8 with $k = s - a$ we obtain $d(\mathcal{C}_A) \geq n(s - a) + 2$, which is the result of [2].

In the next example we consider systems defined by multi-homogeneous polynomials. This is the case of toric variety $X = \mathbb{P}^1 \times \cdots \times \mathbb{P}^1$.

Example 4.2. For $1 \leq i \leq n$ let P_i be the lattice box with dimensions (d_{i1}, \dots, d_{in}) , each $d_{ij} \geq 1$. Let S be the solution set of a system $f_1 = \cdots = f_n = 0$ with Newton polytopes P_1, \dots, P_n satisfying assumptions (1)–(3). By Bernstein's theorem $|S| = V(P_1, \dots, P_n)$ which equals $\text{Perm}(D)$, the permanent of the matrix $D = (d_{ij})$. Indeed, since each P_i is the Minkowski sum of segments $P_i = \sum_{j=1}^n I_{ij}$, where $I_{ij} = [0, d_{ij}e_j]$, by the multi-linearity of the mixed volume we obtain

$$V(P_1, \dots, P_n) = V\left(\sum_{j=1}^n I_{1j}, \dots, \sum_{j=1}^n I_{nj}\right) = \sum_{\sigma \in S_n} V(I_{1\sigma(1)}, \dots, I_{n\sigma(n)}) = \sum_{\sigma \in S_n} d_{1\sigma(1)} \cdots d_{n\sigma(n)}.$$

Now let A be a lattice box with dimensions (a_1, \dots, a_n) . Note that P is a lattice box with dimensions (d_1, \dots, d_n) , where $d_j = \sum_i d_{ij}$. Hence A lies in P° whenever $1 \leq a_j \leq d_j - 2$. Next, suppose S satisfies the assumption (4) with $Q = \square$, the unit n -cube. Then for $k = \min_j (d_j - 2 - a_j)$ we have $A + k\square \subset P^\circ$. Applying Theorem 3.8 we get

$$d(\mathcal{C}_A) \geq (2^n - 1) \min_{1 \leq j \leq n} (d_j - 2 - a_j) + 2.$$

Let us now see under which condition on the polytopes P_i the assumption (4) is generically satisfied. According to Theorem 3.9 it is enough to require $V(P_1, \dots, P_{n-1}, \square) \geq 2^n$ and $(2^n - 1)\square \subset P_n$. The latter occurs when $d_{nj} \geq 2^n - 1$ for $1 \leq j \leq n$. For the former note that $\square \subset P_i$, so by monotonicity of the mixed volume

$$V(P_1, \dots, P_{n-1}, \square) \geq V(\square, \dots, \square) = n! \geq 2^n,$$

for $n \geq 4$. For $n = 2$ we require $V(P_1, \square) = d_{11} + d_{12} \geq 4$. For $n = 3$ we require that at least one edge of either P_1 or P_2 has length 2, since in this case

$$V(P_1, P_2, \square) = d_{11}d_{22} + d_{12}d_{23} + d_{13}d_{21} + d_{13}d_{22} + d_{12}d_{21} + d_{11}d_{23} \geq 8.$$

Here is a small example of a toric complete intersection code over \mathbb{F}_{13} .

Example 4.3. Let P_1 and P_2 be as in Figure 4.1.

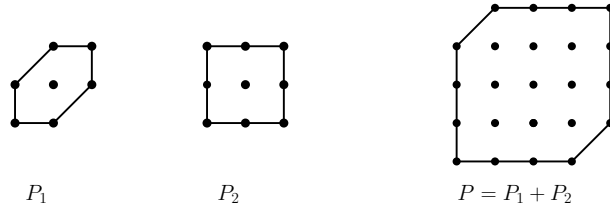


FIGURE 4.1. The Newton polygons and their Minkowski sum

Consider the system

$$\begin{cases} f_1 = 1 - 6x + 2y - 4xy + 4x^2y - 2xy^2 - x^2y^2 = 0 \\ f_2 = 1 + 2x + y - x^2 - 2xy - y^2 + 3x^2y + 4xy^2 + 2x^2y^2 = 0. \end{cases}$$

The system has $8 = V(P_1, P_2)$ simple solutions in $(\mathbb{F}_{13}^*)^2$:

$$S = \{(-6, -4), (-6, -3), (-4, -1), (-2, -5), (-2, -4), (1, 2), (5, 5), (6, 1)\}.$$

Let $Q = \square$, the unit square. One can check that any 4 points of S impose independent conditions on the space $\mathcal{L}(Q)$. Now choose $A = \square$ as well. We have $A + \square \subset P^\circ$, so

$$d(\mathcal{C}_A) \geq (4 - 1) + 2 = 5.$$

Furthermore $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| = 4$, so we get an MDS $[8, 4, 5]$ -code over \mathbb{F}_{13} .

To construct a bigger example we start with polygons P_1, P_2 satisfying the conditions of Theorem 3.9. Then we choose a random polynomial f_1 with Newton polytope P_1 . If the size of the field is big enough we can choose $V(P_1, P_2)$ rational points on the curve $f_1 = 0$ which satisfy assumption (4).

Example 4.4. The polygons P_1 and P_2 and their Minkowski sum P are depicted in Figure 4.2. Let S be a solution set of $f_1 = f_2 = 0$ with Newton polytopes P_1, P_2 satisfying assumptions (1)–(3). We have $|S| = V(P_1, P_2) = 16$.

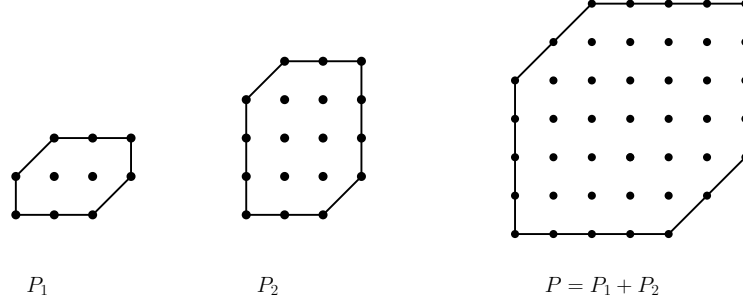


FIGURE 4.2. The Newton polygons and their Minkowski sum

Here is an application of Theorem 3.2. Take A to be a 2×2 lattice square, Δ_1 the convex hull of $\{(0, 0), (1, 0), (1, 1)\}$, and Δ_2 the convex hull of $\{(0, 0), (0, 1), (1, 1)\}$. Then $A + \Delta_1 + \Delta_2 \subset P^\circ$. Therefore, by Theorem 3.2, we have $d(\mathcal{C}_A) \geq 2 + 2 = 4$. For fields of more than 3 elements the evaluation map $\text{ev}_S : \mathcal{L}(A) \rightarrow \mathbb{F}_q^{16}$ is injective, hence $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| = 9$ and we obtain a $[16, 9, \geq 4]$ -code over \mathbb{F}_q with $q \geq 4$.

Next we consider a set S satisfying the additional assumption (4). We set $Q = \square$, the unit square. Since $V(P_1, \square) = 5 \geq 4$ the first condition of Theorem 3.9 is satisfied. By Remark 3.10 we can replace the second condition with $\bar{P} \subset P_2$, where \bar{P} is the union of $(P_1 + \square)^\circ$ and $P(J_f^T)$, the Newton polytope of the Jacobian of (f_1, h) where the Newton polytopes of f_1 and h are P_1 and \square , respectively. It is easy to see that $\bar{P}_{\mathbb{Z}}$ is a 2×3 grid of lattice points which is contained in P_2 after a lattice translation.

Here is a random polynomial over \mathbb{F}_{73} with Newton polytope P_1 :

$$f_1 = 1 + 3x^2 + 7y - 11xy + 13x^2y - 12x^3y - 4xy^2 + 7x^2y^2 - 26x^3y^2.$$

The following set S of \mathbb{F}_{73} -rational zeroes of f_1 imposes independent conditions on $\mathcal{L}(Q)$:

$$S = \{(17, 16), (-27, 27), (28, -26), (13, -36), (-13, 11), (-28, 21), (-23, 22), (-9, 23), \\ (-14, 27), (-36, 13), (12, 30), (23, 11), (3, 15), (-12, -20), (-35, 9), (-18, 16)\}.$$

Since $|P_2 \cap \mathbb{Z}^2| > |S| = 16$ there exist polynomials f_2 with Newton polytope P_2 which vanish at S . For example we can take

$$f_2 = -13 + 34x^2 - 2y - 3xy + 25x^2y + 10x^3 - 20y^2 + 22xy^2 + 13x^2y^2 \\ + 25y^3 + xy^3 + 2x^2y^3 + 17xy^4 + 25x^2y^4 + x^3y^4.$$

By Bernstein's theorem S is the solution set of $f_1 = f_2 = 0$ and satisfied assumptions (1)–(4). Next we look at different choices of the set A .

- (a) Let A be the small hexagon from Figure 4.1. Then $A + 2\Box \subset P^\circ$, so by Theorem 3.8 we get $d(\mathcal{C}_A) \geq (4 - 1) \cdot 2 + 2 = 8$. It is easy to see that $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| = 7$ and we obtain a $[16, 7, \geq 8]$ -code over \mathbb{F}_{73} .
- (b) Let A be the segment joining $(0, 0)$ and $(1, 1)$. Then $A + 3\Box \subset P^\circ$, so by Theorem 3.8 we get $d(\mathcal{C}_A) \geq (4 - 1) \cdot 3 + 2 = 11$. Since $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| = 2$ we get a $[16, 2, \geq 11]$ -code over \mathbb{F}_{73} .
- (c) Let A be the Minkowski sum of the small hexagon from Figure 4.1 and the unit square. Then $A + \Box \subset P^\circ$ so by Theorem 3.8 we get $d(\mathcal{C}_A) \geq (4 - 1) + 2 = 5$. To compute the dimension of \mathcal{C}_A note that $\text{ev}_S : \mathcal{L}(A) \rightarrow \mathbb{F}_{73}^{16}$ has 2-dimensional kernel. In fact, $\mathcal{L}(A) \cap I = \text{span}\{f_1, xf_1\}$, where I is the ideal generated by f_1, f_2 . Therefore $\dim \mathcal{C}_A = |A_{\mathbb{Z}}| - 2 = 12$. This shows that \mathcal{C}_A is an MDS code over \mathbb{F}_{73} with parameters $[16, 12, 5]$.

5. CONCLUSION AND FURTHER WORK

Given a system of Laurent polynomial equations $f_1 = \dots = f_n = 0$ with n -dimensional Newton polytopes P_1, \dots, P_n satisfying assumptions (1)–(3) or (1)–(4) and a set $A \subset P^\circ$ we found lower bounds for the minimum distance of the evaluation code \mathcal{C}_A . As of the moment, over fields of positive characteristic these bounds hold when the polytopes P_i have the same collection of facet normals (see the discussion at the beginning of Section 2.2). We would like to remove or weaken this assumption.

Furthermore, when constructing a toric complete intersection code in Example 4.4 we were choosing random coefficients in a sufficiently large finite field. We would like to find a way of constructing toric complete intersection codes that works for smaller fields as well.

Computing the dimension of \mathcal{C}_A is not obvious since the evaluation map will have a non-trivial kernel, in general. It requires computing the codimension of the ideal generated by the f_i in the space $\mathcal{L}(A)$. Although this can be done in concrete examples one would like to have a general way of doing so.

REFERENCES

- [1] D. N. Bernstein, *The number of roots of a system of equations*, Funct. Anal. and Appl. **9** (2) (1975), 183–185.
- [2] E. Ballico, C. Fontanari, *The Horace method for error-correcting codes*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 2, 135139.
- [3] E. Cattani, D. Cox, A. Dickenstein, *Residues in Toric Varieties*, Compositio Math. **108** (1997), no. 1, 35–76.
- [4] E. Cattani, A. Dickenstein, *A global view of residues in the torus*, J. Pure Appl. Algebra **117/118** (1997), 119–144.
- [5] D. A. Cox, *Toric residues*, Arkiv für Matematik **34** (1996) 73–96.
- [6] I. Duursma, C. Rentería, H. Tapia-Recillas, *Reed-Muller codes on complete intersections*, Appl. Algebra Engrg. Comm. Comput. **11** (2001), 455–462.

- [7] D. Eisenbud, M. Green, J. Harris, *Cayley–Bacharach theorems and conjectures*, Bull. Amer. Math. Soc. **33** (1996), no. 3, 295–324.
- [8] W. Fulton, *Introduction to Toric Varieties*, Princeton Univ. Press, Princeton, 1993
- [9] O. A. Gelfond, A. G. Khovanskii, *Toric geometry and Grothendieck residues*, Moscow Math. J. **2** (2002), no. 1, 99–112.
- [10] L. Gold, J. Little, H. Schenck, *Cayley–Bacharach and evaluation codes on complete intersections*, J. Pure Appl. Algebra **196** (2005), no. 1, 91–99.
- [11] J. Hansen, *Linkage and codes on complete intersections*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), 175–185.
- [12] J. Hansen, *Error-Correcting Codes from Higher-Dimensional Varieties*, Finite Fields and Their Applications, **7** (2001) no. 4, 530–552.
- [13] J. Hansen, *Toric Surfaces and Error-correcting Codes* in Coding Theory, Cryptography, and Related Areas, Springer (2000), pp. 132–142.
- [14] R. Joshua, R. Akhtar, *Toric residue codes: I*, Finite Fields Appl. **17** (2011), no. 1, 1550.
- [15] D. Joyner, *Toric codes over finite fields*, Appl. Algebra Engrg. Comm. Comput., **15** (2004), pp. 63–79.
- [16] A. G. Khovanskii, *Newton polyhedra and the Euler–Jacobi formula*, Russian Math. Surveys **33:6** (1978), 237–238.
- [17] E. Kunz, *Residues and duality for projective algebraic varieties*, University Lecture Series, **47**, AMS, Providence, RI, (2008).
- [18] A. G. Kushnirenko, *Newton polyhedra and Bezout’s theorem* (Russian) Funkcional. Anal. i Prilozhen. **10** (1976), no. 3, 82–83.
- [19] J. Little, *Algebraic geometry codes from higher dimensional varieties*, arXiv:0802.2349v1
- [20] J. Little, H. Schenck, *Toric Surface Codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), no. 4, 999–1014.
- [21] J. Little, R. Schwarz, *On toric codes and multivariate Vandermonde matrices*, Appl. Algebra Engrg. Comm. Comput. **18** (4) (2007), pp. 349–367.
- [22] Diego Ruano, *On the parameters of r -dimensional toric codes*, Finite Fields and Their Applications **13** (2007), pp. 962–976.
- [23] I. Soprunov, *Global residues for sparse polynomial systems*, J. Pure Appl. Algebra **209** (2007), no. 2, 383–392.
- [24] I. Soprunov, J. Soprunova, *Toric surface codes and Minkowski length of polygons*, SIAM J. Discrete Math. **23**, Issue 1, (2009) pp. 384–400
- [25] I. Soprunov, J. Soprunova, *Bringing Toric Codes to the next dimension*, SIAM J. Discrete Math. **24**, Issue 2, (2010) pp. 655–665
- [26] Ștefan O. Tohaneanu, *Lower bounds on minimal distance of evaluation codes*, Appl. Algebra Engrg. Comm. Comput. **20** (2009), no. 5–6, 351–360
- [27] Ștefan O. Tohaneanu, *The minimum distance of sets of points and the minimum socle degree*, J. Pure Appl. Algebra **215** (2011), no. 11, 2645–2651.
- [28] M. Tsfasman, S. Vlăduț, *Algebraic-geometric codes*, Kluwer, Dordrecht, (1991).
- [29] Jan Tuitman, *Counting points in families of nondegenerate curves*, Ph.D. thesis, (2010)